What is Claimed:

1. A system for providing a computing environment, the environment including a virtual memory, the system comprising:

a virtual memory manager that provides the virtual memory by moving or copying data between a volatile memory and a paging file stored in a hard disk, the system protecting the contents of the virtual memory by encrypting the data stored in the paging file.

2. The system of claim 1, wherein the virtual memory manager communicates the data to a file system, wherein the file system causes the data to be encrypted prior to storing the data in the paging file.

3. The system of claim 2, wherein the file system marks the paging file for encryption, and wherein the paging file, upon receiving a request to store the data in the paging file, determines that the paging file has been marked for encryption and communicates with an encryption component to encrypt the data.

4. The system of claim 1, further comprising a key generator that generates a session key, the session key being used to encrypt the data, and the session key being further needed for subsequent decryption of the encrypted data.

5. The system of claim 4, wherein the session key is non-persistently stored in a manner that causes the session key to become unavailable in the event that a boot occurs after generation of the session key.

6. The system of claim 5, wherein the system further protects the contents of the virtual memory by ensuring that there is no persistent storage of the session key.

7. The system of claim 1, wherein encryption of the data is performed according to one or more of the following algorithms:

Data Encryption Standard (DES);

Triple-DES (3DES); or

Advanced Encryption Standard (AES).

8. The system of claim 1, wherein the system further protects the contents of the virtual memory by ensuring that all user mode applications and data that are stored in the virtual memory are encrypted when being stored in the paging file.

9. A method of protecting a virtual memory comprising:

storing data in a plurality of pages of a volatile memory;

determining to move contents of a first one of said plurality of pages from said volatile memory to a paging file stored on a disk;

providing said contents to a file system with instructions to store said contents in a paging file, said paging file being marked for encryption, said file system causing said contents to be encrypted with a key prior to storing said contents in said paging file, said key being required to decrypt information contained in said paging file, said key being stored in a manner such that a reboot of a machine on which said key is stored causes said key to be lost.

10. The method of claim 9, further comprising:

generating said key upon a boot of said machine.

11. The method of claim 9, further comprising:

prior to generation of said key, reserving a block of said volatile memory for use as a workspace, whereby use of the workspace avoids the need to copy volatile memory contents to disk prior to generation of the session key.

12. The method of claim 9, wherein the file system causes said contents to be encryption by communicating with an encryption component, the encryption component encrypting files that have been marked by the file system for encryption.

13. The method of claim 12, further comprising:

reserving a block of said volatile memory in which data may be passed back and forth between the file system and the encryption component.

14. A system for maintaining an encrypted paging file that stores virtual memory data for a computer, the system comprising:

an encryption component that receives data and performs encryption and decryption operations on said data using a key;

a mechanism that generates said key;

a storage location in the computer that stores said key in a manner that causes said key not to persist across boots of the computer; and

a virtual memory manager that copies or moves data from volatile memory to disk by requesting that a file system store the copied or moved data in a paging file, the file system calling upon the encryption component to encrypt the copied or moved data with said key.

15. The system of claim 14, wherein the encryption component reserves a block of memory upon startup.

16. The system of claim 15, wherein the block of memory is used as a workspace for the encryption component prior to generation of said key, whereby sufficient space for storage of said encryption component's operating data exists in said volatile memory prior to generation of said key.

17. The system of claim 15, wherein the block of memory is used as a buffer to pass information between the file system and the encryption component.

18. The system of claim 14, wherein said key is generated before said virtual memory manager directs the storage of data into the paging file.

19. The system of claim 14, wherein said key is stored in said volatile memory, and wherein no copy of said key is stored in any non-volatile memory or storage device of the computer.

20. A computer-readable medium encoded with computer executable instructions to perform a method that takes place upon startup of a computer, the method comprising:

generating a session key;

storing said session key in a non-persistent manner that does not survive across machine boots;

retrieving information indicating that virtual memory data stored on disk is to be encrypted;

marking a paging file as an encrypted file;

receiving, from a memory manager, data from a volatile storage device that is to be stored on disk in the paging file; and

protecting the received data from observation by encrypting the received data with a session key prior to storing said data in the paging file.

21. The computer-readable medium of claim 20, wherein the method further comprises:

reserving a block of memory prior to generation of the session key, wherein the block of memory is used either as:

a buffer to pass data between a file system that maintains the paging file and an encryption component that performs encryption and decryption of the data with the session key; and

a workspace usable by the encryption component prior to generation of the session key.

22. The computer-readable medium of claim 20, wherein the session key is stored in the volatile storage device, and no copy of the session key is stored on disk.

23. A method of protecting a virtual memory comprising:

storing data in a plurality of pages of a volatile memory;

determining to move contents of a first one of said plurality of pages from said volatile memory to a paging file stored on a disk;

providing said contents to a file system with instructions to store said contents in a

paging file, said paging file being marked for encryption, said file system causing said contents to be encrypted with a key prior to storing said contents in said paging file, said key being required to decrypt information contained in said paging file, said key being stored in a manner such that a reboot of a machine on which said key is stored causes said key to be lost.